Correlation between NetFlow System and Network Views for Intrusion Detection

Cristina Abad, Yifan Li*, Kiran Lakkaraju, Xiaoxin Yin and William Yurcik

Presented by

Yifan Li

National Center for Supercomputing Applications (NCSA)

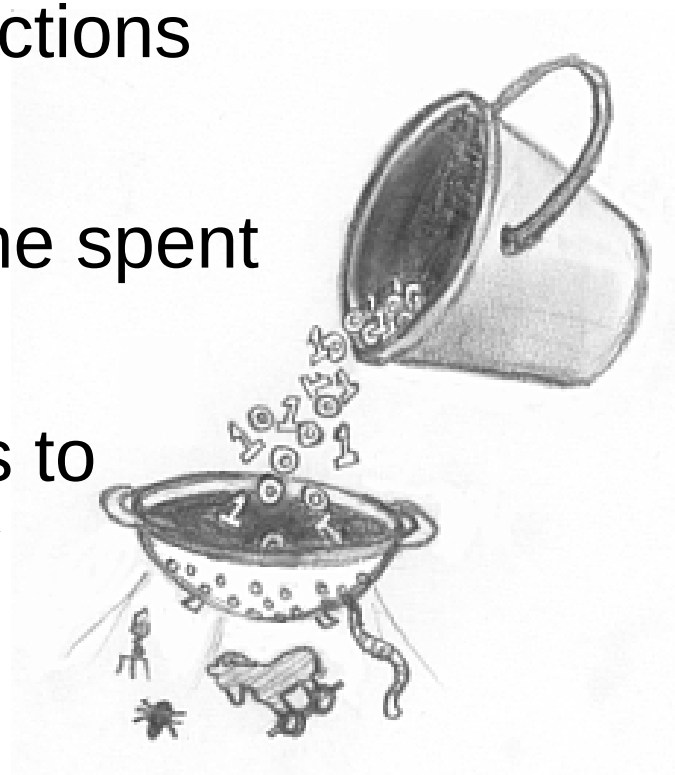
University of Illinois at Urbana-Champaign

On Intrusion Detection

- IDSs are important to protect networked systems
- However, intrusion detection is difficult:
  - many attacks, new attacks, changing all the time
  - poor performance (false positives)
  - information overload to human users
  - scalability (huge data volume, data management)
  - many logs, each with different purposes and formats

Information Visualization for Intrusion Detection

- Leverage human cognitive abilities
- Promotes quick mental connections between security events
- Help reduce the amount of time spent tracing attacks
- Allows less experienced users to better understand the security events



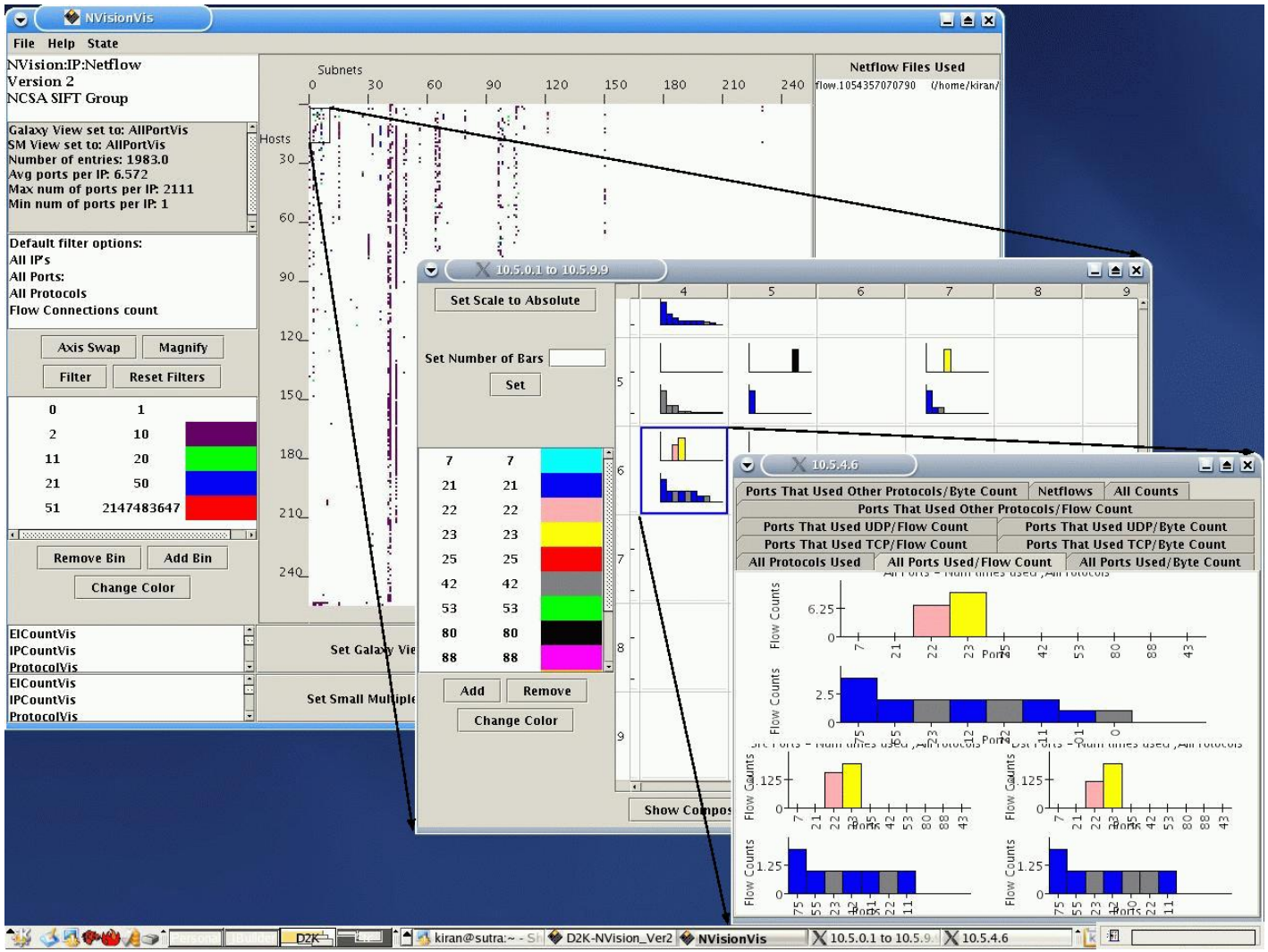
Visualizing NetFlows

- NetFlows: obtained by hardware (Cisco) or software (Argus)
- Contain summarized traffic information
- We visually represent them in two views:
  - System
    - NVisionIP
  - Network
    - VisFlowConnect
- Correlating information presented in both enhances the intrusion detection process

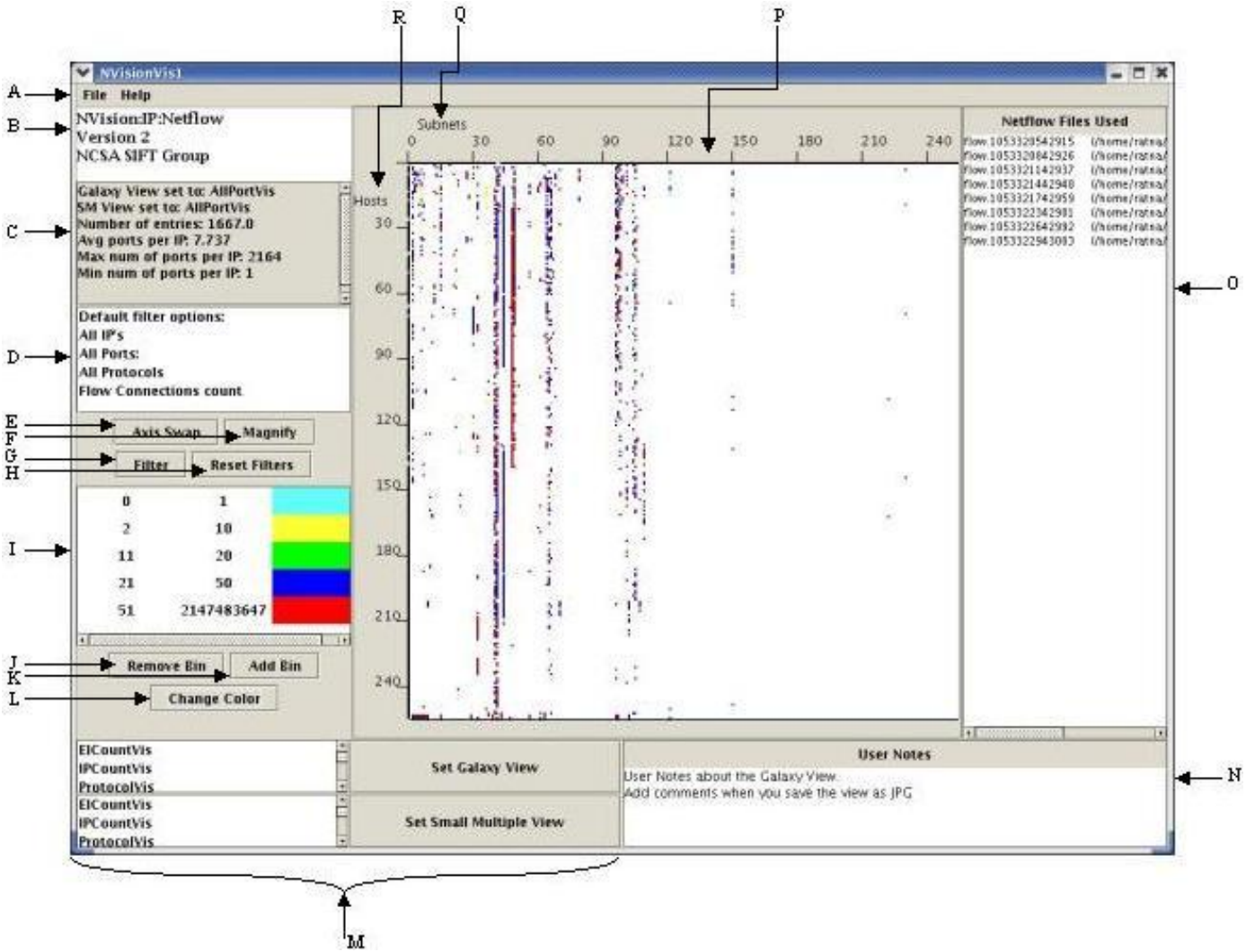
NVisionIP System Views

- Built within D2K (Data-to-Knowledge)
- Three main views:
  - Galaxy View
  - Small Multiple View
  - Machine View
- Statistical information is collected for each host
- Extensive filtering capabilities

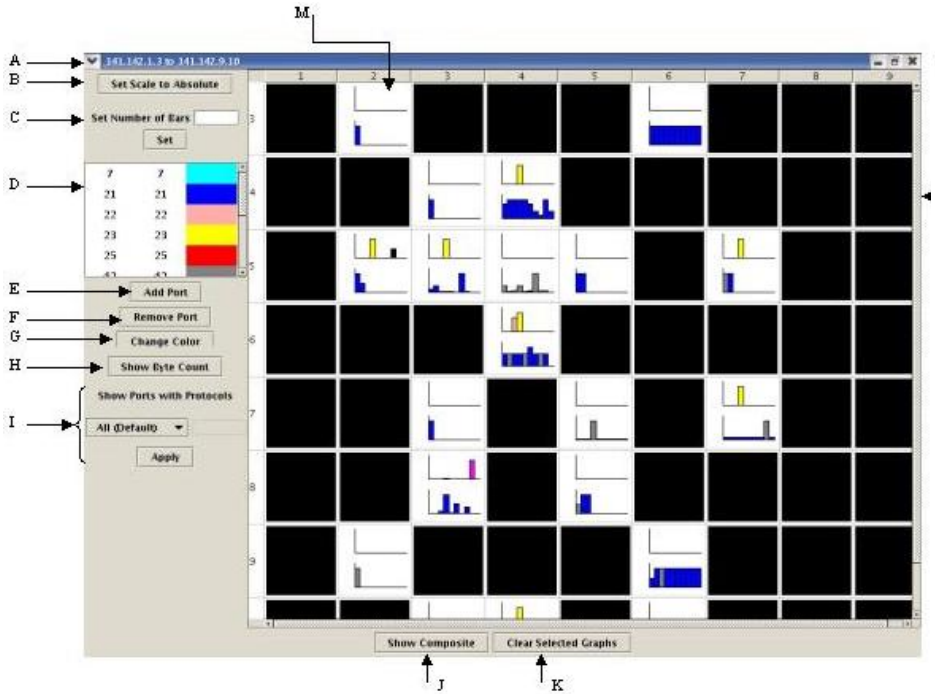
NVisionIP

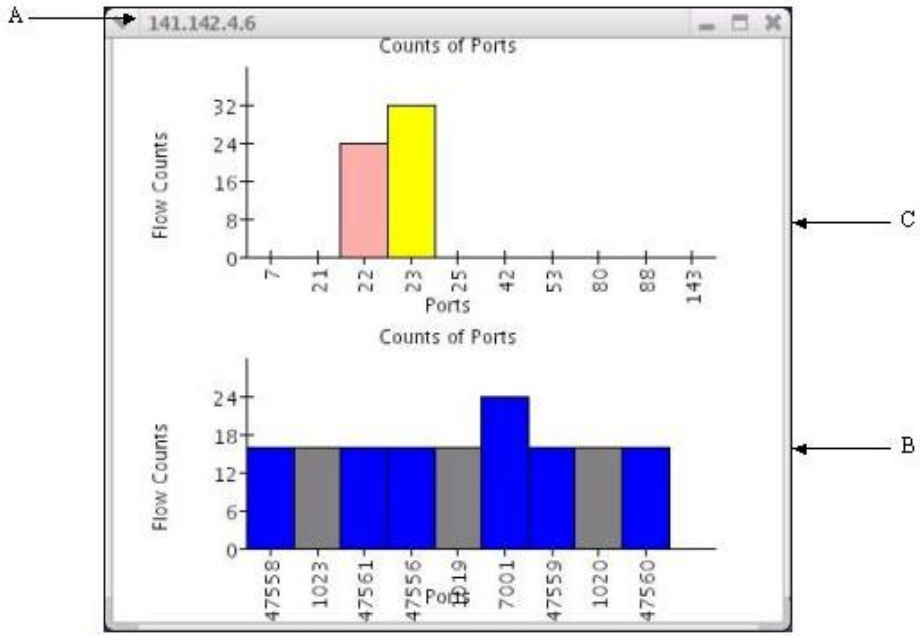

NVisionVis
File Help State
NVision:IP:Netflow
Version 2
NCSA SIFT Group
Galaxy View set to: AllPortVis
SM View set to: AllPortVis
Number of entries: 1983.0
Avg ports per IP: 6.572
Max num of ports per IP: 2111
Min num of ports per IP: 1
Default filter options:
All IP's
All Ports:
All Protocols
Flow Connections count
Axis Swap
Magnify
Filter
Reset Filters
Remove Bin
Add Bin
Change Color
Subnets
Hosts
Netflow Files Used
10.5.0.1 to 10.5.9.9
Set Scale to Absolute
Set Number of Bars
Set
Add
Remove
Change Color
10.5.4.6
Ports That Used Other Protocols/Byte Count
Netflows
All Counts
Ports That Used Other Protocols/Flow Count
Ports That Used UDP/Flow Count
Ports That Used UDP/Byte Count
Ports That Used TCP/Flow Count
Ports That Used TCP/Byte Count
All Protocols Used
All Ports Used/Flow Count
All Ports Used/Byte Count
Flow Counts
Ports

Galaxy View


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
NVisionVis1
File Help
NVision:IP:Netflow
Version 2
NCSA SIFT Group
Galaxy View set to: AllPortVis
SM View set to: AllPortVis
Number of entries: 1667.0
Avg ports per IP: 7.737
Max num of ports per IP: 2164
Min num of ports per IP: 1
Default filter options:
All IP's
All Ports:
All Protocols
Flow Connections count
Axis Swap
Magnify
Filter
Reset Filters
0 1
2 10
11 20
21 50
51 2147483647
Remove Bin
Add Bin
Change Color
Subnets
Hosts
Netflow Files Used
ElCountVis
IPCountVis
ProtocolVis
ElCountVis
IPCountVis
ProtocolVis
Set Galaxy View
Set Small Multiple View
User Notes
User Notes about the Galaxy View
Add comments when you save the view as JPG

Small Multiple View and Machine View

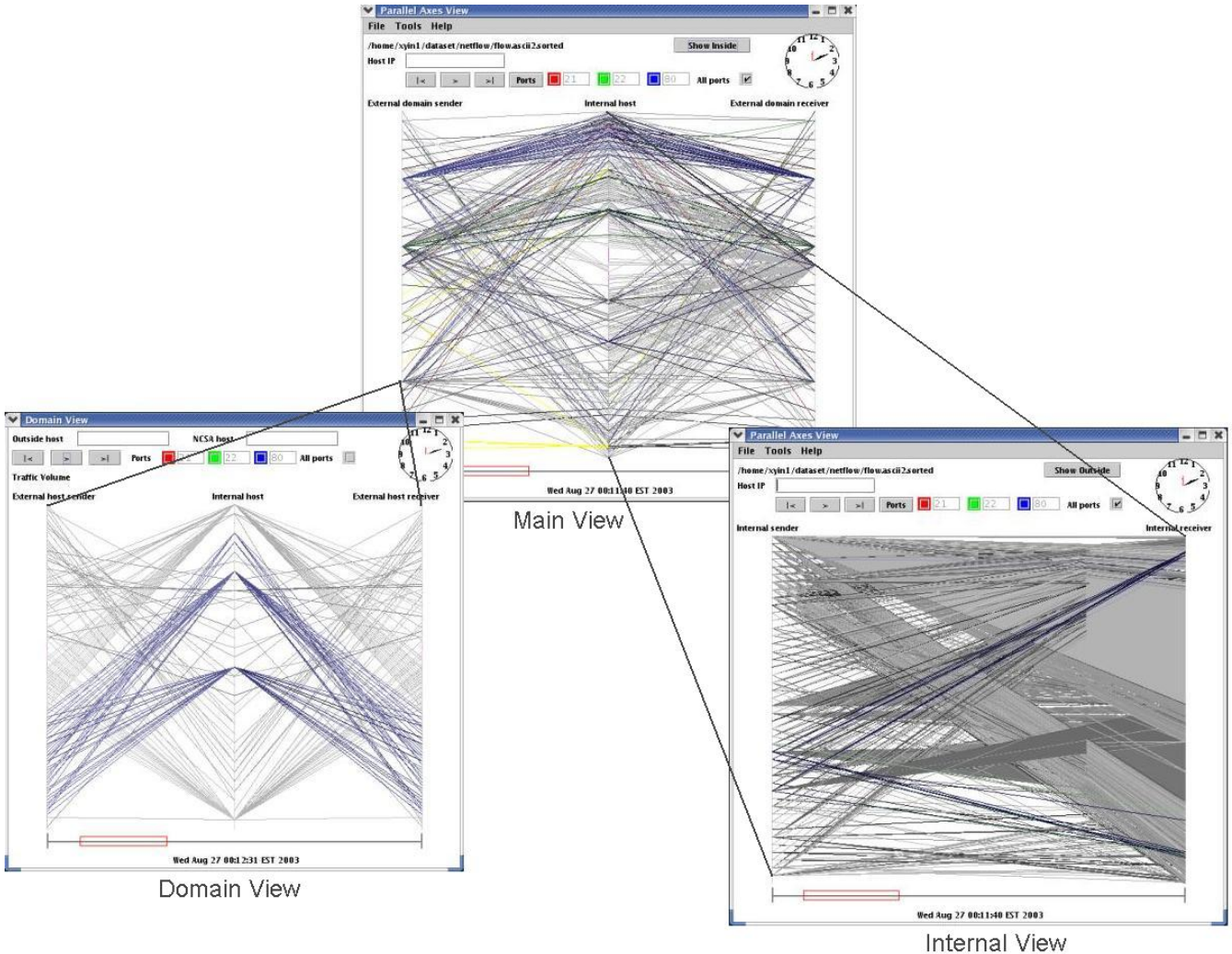




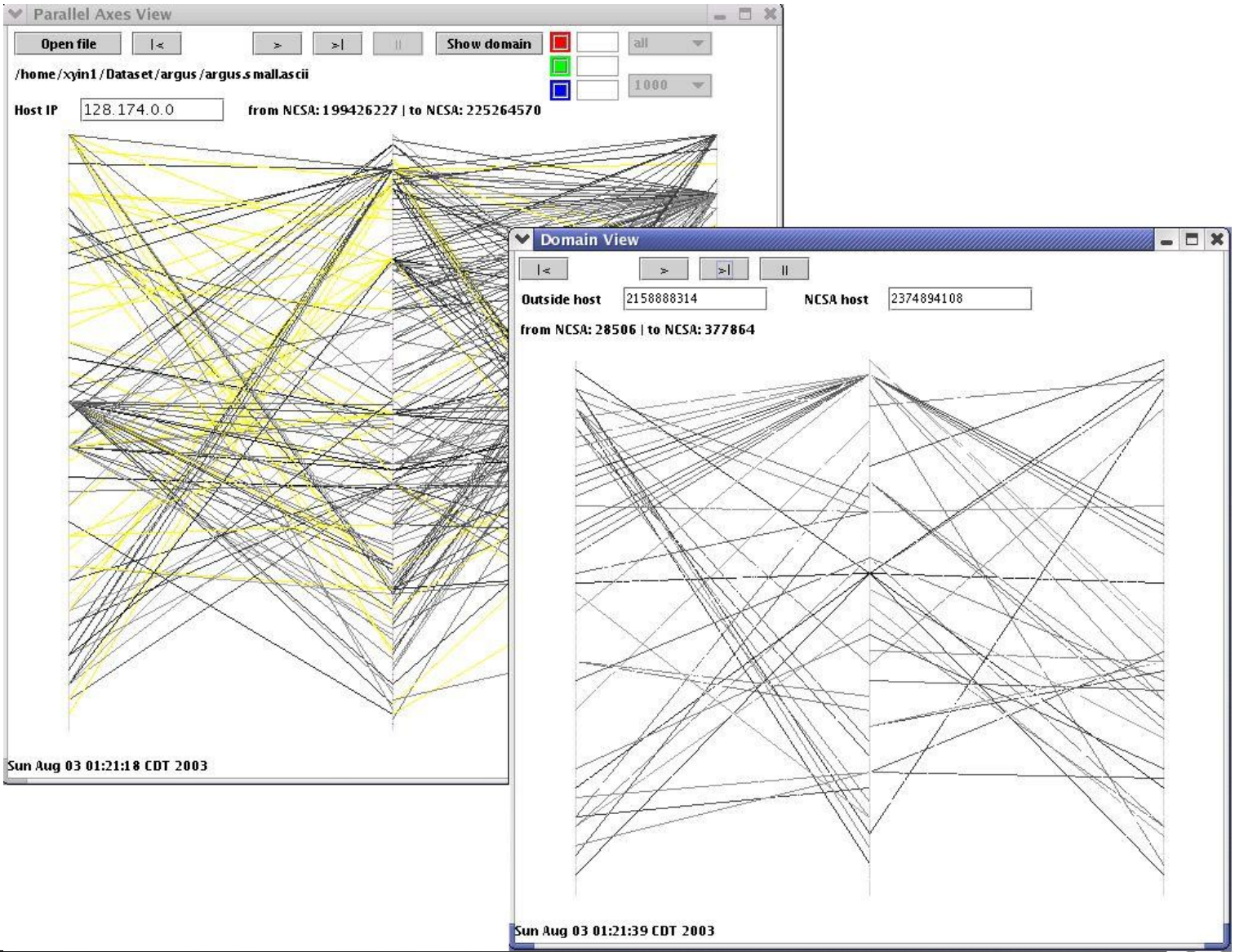
VisFlowConnect Network Views

- Visualize information between hosts:
  - Internal – External
  - Internal – Internal
- A point in each axes represents a host or a subnet
- Displays *to* and *from* traffic
- Extensive filtering capabilities
- Traffic pattern changes can be easily identified
- Animation

VisFlowConnect



Main View and Domain View



Enhancing the Intrusion Detection Process

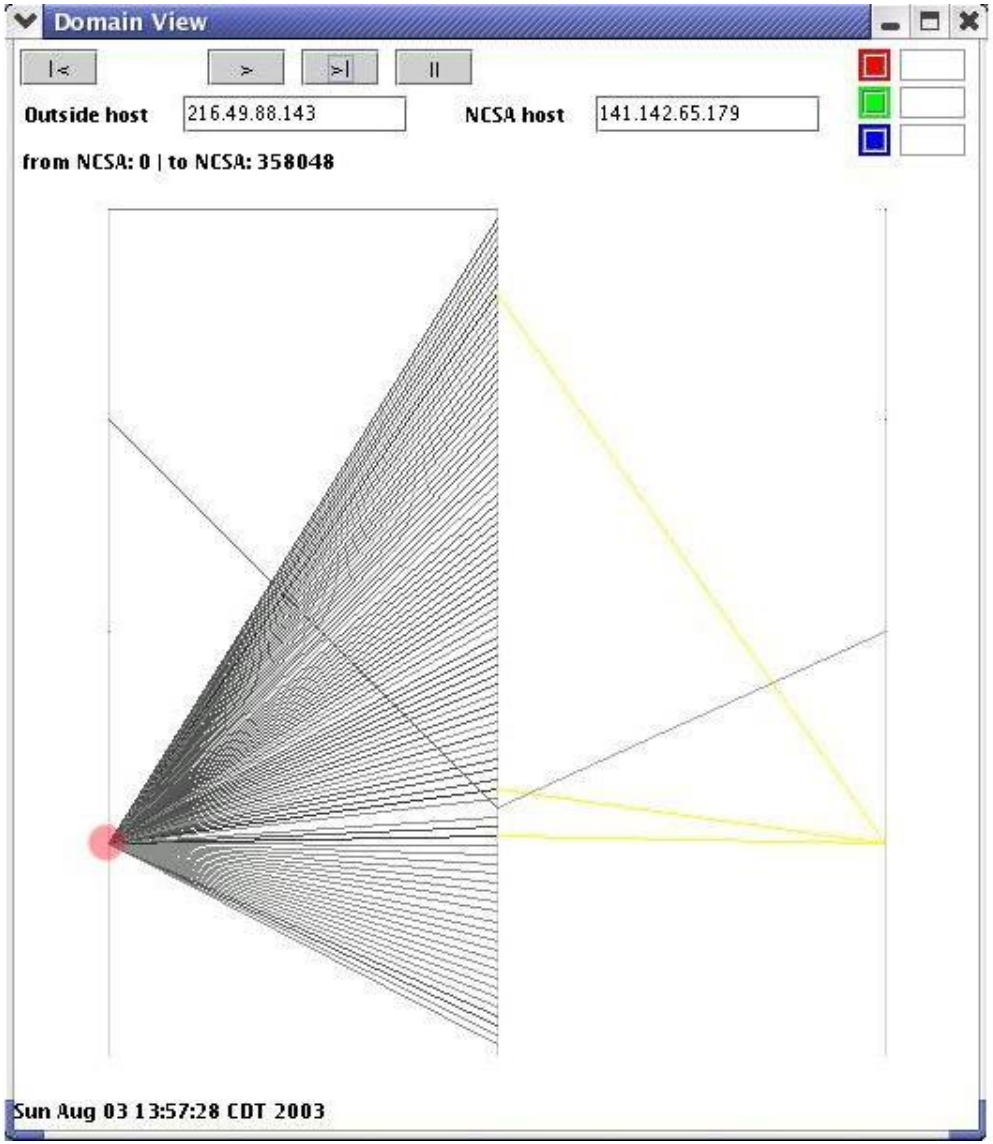
NVisionIP

- Visualize pattern changes
- Filter anomalous IP/subnet
- Filter particular port
- Visualize activity on unusual ports

VisFlowConnect

- One-to-many
- Many-to-one
- Increased bandwidth consumption
- Asymmetry
- Pattern changes

One-to-Many Pattern



Combination of the Tools

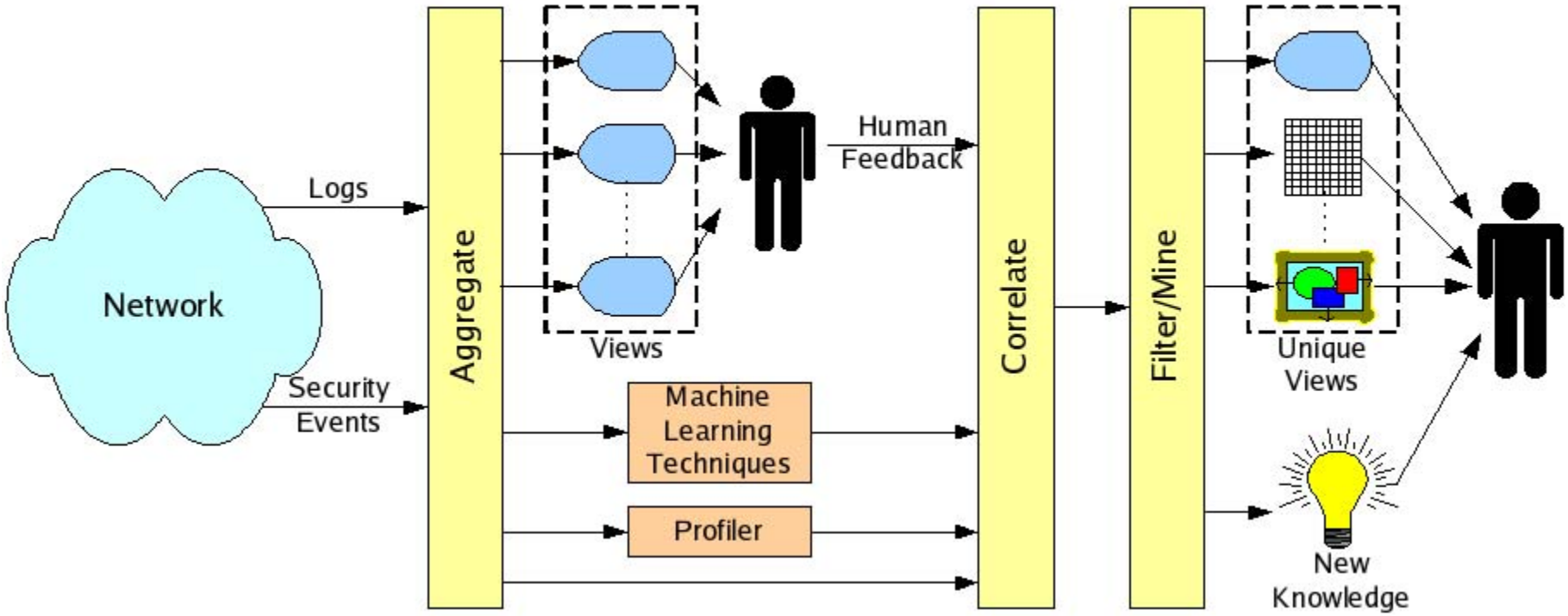
- What can we say about the figure?
  - Malicious scan?
  - Known software to help find vulnerabilities of the system?
- Use NVisionIP
  - Filter out those known ports
- More in the paper …

Link Analysis & Our Work

- Reveals complex patterns of correlations between individual values
  - understand the hidden structure of investigated data
  - isolate interested patterns for further investigation

- NVisionIP and VisFlowConnect
  - only significant links shown
  - interesting patterns identified

Future Work


Network
Logs
Security
Events
Aggregate
Views
Human
Feedback
Machine
Learning
Techniques
Profiler
Correlate
Filter/Mine
Unique
Views
New
Knowledge

Questions?

http://www.ncassr.org